AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Dropbox account associated with the email address [redacted]

Case No. 3:22-mj-106

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A-4

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-4

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
SEE ATTACHMENT C-4	

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Andrea R. Kinzig, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: 3/31/22

City and state: Dayton, OH

Peter B. Silvain, Jr.
United States Magistrate Judge

ATTACHMENT A-4

Information associated with the Dropbox account associated with the email address [redacted] that is stored at premises owned, maintained, controlled, or operated by Dropbox Inc., a company that accepts service of legal process at 1800 Owens Street, San Francisco, California, 94158.

ATTACHMENT B-4

Particular Things to be Seized

I. Information to be disclosed by Dropbox Inc. (the "Provider")

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-4:

a. All available user/subscriber details for the account, including: full name, user identification number, birth date, gender, contact e-mail addresses, passwords, security questions and answers, telephone numbers, screen names, websites, and other personal identifiers;

b. All files downloaded and/or uploaded by the user account, including any deleted files;

c. Logs of IP addresses and devices utilized to access the account;

d. Logs reflecting activity to the account, including information about the account name, computer name, and dates that files were uploaded, deleted, and modified;

e. Records of any Dropbox links posted by the account user, and records of any other users who accessed these links;

f. Records of any Dropbox links accessed by the account user, and records of the original poster of those links;

g. All information related to the account's settings, including but not limited to linked devices, linked Facebook and Twitter accounts, etc.;

h. The length of service (including start date); and

i. Any payment information related to the account, including full credit card numbers.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography.

2. Any images and videos depicting child pornography.

3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

4. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers.

5. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.

6. Any geo-location information for the account or other records reflective of the whereabouts of the account user.

7. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-4

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography offenses committed by [redacted] (hereinafter referred to as [redacted]). This Affidavit is submitted in support of Applications for search warrants for the following:

   a. Information associated with the email account [redacted] that is stored at premises controlled by Yahoo Inc. (as more fully described in Attachment A-1);

   b. Information associated with the Google account [redacted] that is stored at premises controlled by Google LLC (as more fully described in Attachment A-2);

   c. Information associated with the Kik account with the user name of [redacted] that is stored at premises controlled by MediaLab.ai Inc. (as more fully described in Attachment A-3);

   d. Information associated with the Dropbox account associated with the email address [redacted] that is stored at premises controlled by Dropbox Inc. (as more fully described in Attachment A-4); and

   e. Information associated with the Skype accounts containing the user names of [redacted] and [redacted] that is stored at premises controlled by Microsoft Corporation USA (as more fully described in Attachment A-5).

3. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:

a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(2), which make it a crime to possess child pornography; and

b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce.

4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-5 hereto and are incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit is intended to show that there is sufficient probable cause to support the searches of the above noted accounts (as defined in Attachments A-1 through A-5). It does not contain every fact known to the investigation.

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1), are present within the information associated with the above noted accounts (as described in Attachments A-1 through A-5).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States" that "has jurisdiction over the offense being investigated" 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. §§ 2252(a)(2) and (b)(1) state that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such

visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

10. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) state that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

11. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

12. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachments B-1 through B-5 to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8): any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. "**Child erotica**", as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

f. "**Internet Service Providers**" or "**ISPs**" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

g. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is [redacted]. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a

practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

h. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

i. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

j. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

k. "**Social Media**" is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users' account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.

Email Accounts

14. Yahoo Inc. is a company based in Sunnyvale, California. In my training and experience, I have learned that Yahoo Inc. provides a variety of online services, including electronic mail ("email") access, to the public.

15. Yahoo Inc. allows subscribers to obtain email accounts at the domain name yahoo.com and ymail.com, like the account listed in Attachment A-1. Subscribers obtain accounts by registering with Yahoo Inc. During the registration process, Yahoo Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo Inc. subscribers) and information concerning subscribers and their use of Yahoo Inc.

services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. In general, emails that are sent to Yahoo Inc. subscribers are stored in the subscriber's "mail box" on Yahoo Inc.'s servers until the subscriber deletes the email. If the subscriber does not delete the message, the messages can remain on Yahoo Inc.'s servers indefinitely. Even if the subscriber deletes an email, it may continue to be available on Yahoo Inc.'s servers for a certain period of time.

17. Yahoo Inc. subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Yahoo Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

19. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

20. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the

provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

Google Services

22. Google LLC ("Google") is a multi-national corporation with its headquarters located in Mountain View, California. Google offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

23. In addition, Google offers an operating system ("OS") for mobile devices (including cellular phones) known as Android. Google also sells devices, including laptops, mobile phones,

tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

24. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. However, users can also sign up for Google accounts with third-party email addresses.

25. Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below. Google's services include but are not limited to the following:

a. Gmail: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

b. Contacts: Google provides address books for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

c. Calendar: Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in

Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

d. Messaging: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

e. Google Drive: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me". Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

f. Google Keep: Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.

g. Google Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the

option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

h. Google Maps: Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

i. Location History: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

j. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

k. Android Backup: Android device users can use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, call history, contacts, device settings, or SMS messages. Users can also opt-in through Google One to back up photos, videos, and multimedia sent using Messages

26. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

27. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

28. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

29. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

30. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

31. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

32. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

33. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

34. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

35. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Kik Messenger Application

36. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.

37. The Kik messenger application is administered by MediaLab.ai Inc., a company based in Santa Monica, California. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.

38. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. MediaLab.ai Inc. does not verify this information, and as such, users can provide inaccurate information.

39. MediaLab.ai Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, MediaLab.ai Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. MediaLab.ai Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). MediaLab.ai Inc. does not store or maintain chat message content.

40. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.

41. According to its current Law Enforcement Guide, MediaLab.ai Inc. maintains on its servers the following account information for its users:

    a. Basic subscriber data, including the current first and last names and email addresses, links to the most current profile pictures or background photographs, device related information, account creation dates and Kik versions, birthdays and email addresses used to register the accounts, and users' location information (including IP addresses).

b. Transactional chat logs, which are logs of all the messages that users have sent and received, including senders' usernames, receivers' usernames, receivers' group JID's[1], timestamps, IP addresses of the senders, and word counts;

c. Chat platform logs, which are logs of all the media files that users have sent and received, including senders' usernames, receivers' usernames, receivers' JID's, timestamps, IP addresses of the senders, media types, and Content ID's;

d. Photographs and/or videos sent or received by the users for the last 30 days;

e. Roster logs, which are logs of usernames added and blocked by the subject user (including timestamps);

f. Abuse reports, which are transcripts of reported chat histories against the subject user, including the senders' usernames, receivers' usernames, timestamps, actual messages, and content ID's;

g. Email events, which are logs of all the emails that have been associated with a username; and

h. Registration IP's, which are the IP addresses associated to the usernames when the accounts were registered (including the timestamps).

Cloud Storage and Dropbox

42. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:

a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services

1 JID's are unique internal identification numbers associated with users and group chats. They are randomly generated by Kik's internal system.

whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

b. "Cloud computing" is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

c. "Cloud Service Provider" (CSP) is the entity that offers cloud computing services. CSP's offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP's maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP's reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long- term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a "remote computing service." CSP's may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.

d. "Virtual Machine" (VM) is a system where the hardware is virtual rather than physical. Virtualization is a technique whereby special software, called the hypervisor, can run many virtual (rather than physical) machines. The hardware on the single machine is emulated so that each virtual instance of a computer, called a VM, does not require dedicated physical hardware, but each VM believes it has its own hardware. The hypervisor has special access to control all of the virtual guests, but it should also be able to isolate the guests from each other.

e. "NetFlow Records" are collections of network statistics collected by a service provider about traffic flows. A traffic flow is a sequence of data packets from a source to a destination. NetFlow is collected when it is impractical to collect all of the data packets for a flow. Providers may use these logs for quality control, security, or billing. For any particular network flow, NetFlow can include the source and destination IP addresses, network ports, timestamps, and amount of traffic transferred. A provider may only collect a sample of all possible sessions, and may only store the NetFlow for a short time.

43. Dropbox is an on-line service that allows its users to store files on Dropbox Inc.'s servers.

44. In general, providers like Dropbox Inc. ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

45. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

46. Dropbox Inc. provides its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a "sharing link". A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

47. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize cloud storage accounts to store their child pornography files.

Skype

48. Skype owns and operates a communication service that transmits voice calls, video, and messages over the Internet. In May 2011, Skype was acquired by Microsoft Corporation, a company based in Redmond, Washington.

49. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short

message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.

50. Skype may be installed and used on a desktop computer, laptop, tablet, or mobile phone, including those using operating systems from Apple, Blackberry, Google, and Windows.

51. Skype requires users to provide basic contact information to the company during the registration process. This information may include identification data such as name, username, address, telephone number, mobile number, email address, and profile information such as age, gender, country of residence, and language preference.

52. Skype users can elect to make public profile information consisting of images, links to personal web pages, and links to social media websites. Skype users may also subscribe to other Skype users with whom they are interested or associated.

53. When its users communicate with non-Skype users, the company keeps transaction records during the normal course of business commonly referred to as call detail records. These call detail records consist of the date, time, sender, receiver, duration, and contents of phone calls, text messages, and video messages. According to the company, the transactional records are maintained for six months and data files are stored for 30 to 90 days depending on the type of file.

54. In order to use Skype's premium features like voicemail or to make calls to a landline, cellular telephone, or service outside of the Skype network, a customer must either purchase credits or agree to a monthly or otherwise recurring payment option. This necessitates either providing the company with credit card information, including name, billing address, and credit card number, or the use of an online payment processor such as PayPal.

55. Skype retains system information about the types of devices a customer uses to access their service. This can include computer platform and operating system, Internet Protocol (IP) address information, and mobile device information such as device type, manufacturer name, model number, operating system, and cellular service provider.

56. Skype users may elect to import their contacts from email and social media accounts. This contact information can include name, email address, and/or phone numbers.

57. Skype accesses and stores location information regarding its customers. The location information includes Wi-Fi access points when a customer uses Skype from a home or free Wi-Fi spot, global positioning system (GPS) data when a user searches for free Skype Wi-Fi access points, and GPS data when a Skype user shares their location with another user.

58. Skype users can link their social media accounts with the communication provider. These social media accounts may include Microsoft Corporation, LinkedIn, and Twitter. Skype users may also use an associated Microsoft account and other services. These associated

services may include online file storage, Microsoft email services, and/or other Microsoft products or services.

59. Skype also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Skype, including the information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.

60. Skype uses the following terms to describe the data in its possession:

a. Registration Details: This includes information captured at the time the account was created. This may include identification data such as name, username, address, telephone number, mobile number, email address, and profile information such as age, gender, country of residence, language preference, and any user profile information.

b. Billing Address: The billing address provided by the user that is used in conjunction with payment for Skype services.

c. Skype Online Current Subscription List: A list of Skype users currently subscribed to by the user.

d. Purchase History: Financial transactions with Skype including method of payment information and billing address.

e. Skype Out Records: Historical call detail records for calls placed to cellular and landline phone numbers.

f. Skype Online Records: Historical call detail records for calls placed to the Skype number from landline and mobile numbers.

g. Short Message System Records (SMS): Text messages including the content of the messages.

h. Skype Wi-Fi Records: Historical records of connections to Skype Wi-Fi access points.

i. Email and Password Records: Historical records of emails and password change activities.

61. Communication providers such as Microsoft Corporation typically retain additional information about their users' accounts during the normal course of business, such as information about the length of service (including start date), the types of services utilized, and the means and source of any payments associated with the service (including any credit

card or bank account number). In some cases, Skype users may communicate directly with Skype about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Providers like Microsoft Corporation typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

NCMEC and CyberTipline Reports

62. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

63. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the CyberTipline reports. These ICAC's review the CyberTipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

FACTS SUPPORTING PROBABLE CAUSE

CyberTipline Report

64. On or around January 4, 2022, MediaLab.ai Inc. filed a report to NCMEC's CyberTipline regarding suspected child pornography and/or child exploitation files that were located in a Kik account utilizing the user name of [redacted] NCMEC forwarded MediaLab.ai Inc.'s CyberTipline report, along with the suspected child pornography and/or child exploitation files, to the Cuyahoga County ICAC for further investigation. I later obtained and reviewed the CyberTipline Report and the accompanying files as part of the investigation. Below is a summary of some of the information contained in the report:

a. The [redacted] account was associated with the email address [redacted].

b. Approximately five videos depicting suspected child pornography and/or child exploitation material were located in the [redacted] account (two of which were

duplicates). The report identified that the approximately five videos were sent by the [redacted] user to one (or more) other user(s) via private chat messages.

c. The CyberTipline report indicated that MediaLab.ai Inc. discovered the approximately five video files in the [redacted] account on or around December 27, 2021.

d. Based on my review of the files and my training and experience, I believe that at least approximately two of the videos reported in the CyberTipline report depict child pornography. The other three files (two of which are duplicates) depict adolescent children or young adults engaged in sexually explicit conduct. Based on the characteristics of these individuals, I am unable to determine at this time if they are minors and if the files depict child pornography. The two files depicting child pornography are described as follows:

i. [redacted]

ii. [redacted]

65. As part of filing the CyberTipline report, MediaLab.ai Inc. provided the subscriber information for the [redacted] account as well as the log of IP addresses that were utilized to access the account. These records provided the following information:

a. The [redacted] account was created on or around October 19, 2021. The profile name for the account was [redacted]

b. The email address of [redacted] was associated with the account profile.

c. The account was last accessed on or around January 4, 2021.

d. An iPhone was utilized to access the account on or around December 13, 2021.

e. The log of IP addresses identified that the following IP addresses had been utilized to access the account during the approximate time period of December 5, 2021 through January 4, 2021:

i. The IP address of [redacted] (the IP address utilized to distribute the two child pornography files detailed above) was utilized to access the account on approximately 348 occasions. I have determined that this IP address is serviced by Charter Communications.

ii. The IP address of [redacted] was utilized to access the account on approximately 67 occasions, only during the approximate time period of December 18, 2021 through December 21, 2021. I have determined that this IP address is serviced by Servicio Di Telecomunicacion Di Aruba (Setar) N.V. Based on Internet research, this company is a telecommunications provider in Aruba. The company manages IP addresses for organizations including Marriott Aruba Resort Casino and the Aruba Airport.

iii. The IP addresses [redacted] were utilized to access the account on approximately five occasions on or around December 6, 2021. As of this time, I have not determined who the provider is for these two IP addresses.

iv. Various IP addresses serviced by the Verizon cellular telephone network were utilized to access the account on approximately 543 occasions.

Subpoenaed Records

66. On or around March 7, 2022, an FBI investigator served Charter Communications with an administrative subpoena requesting subscriber information for the IP address of [redacted] on a sample of four of the dates and times it was utilized to access the [redacted] account (including the date and time it was used to send the two child pornography files). Records received from Charter Communications in response to the subpoena identified that during each of the dates and times noted in the subpoena, this IP address was subscribed to [redacted] at [redacted] (hereinafter referred to as the "SUBJECT PREMISES").

67. On or around March 7, 2022, an FBI investigator served Yahoo Inc. with an administrative subpoena requesting subscriber information for the [redacted] email account as well as the log of IP addresses that were utilized to access the account during the time period of January 1, 2021 through March 7, 2022. Records received from Yahoo Inc. in response to the subpoena included the following information:

a. The [redacted] account was created on or around July 17, 2014. The user name for the account was [redacted]

b. The telephone number of [redacted] was associated with the account. The records identified that this telephone number had been verified by a representative of Yahoo Inc.

c. The account was last accessed on or around March 2, 2022, and it was active as of the date of the subpoena.

d. The log of IP addresses identified that the following IP addresses were utilized to access the account:

i. The IP address of [redacted] (the IP address utilized to distribute the two child pornography files detailed above, which is subscribed to [redacted] at the SUBJECT PREMISES) was utilized to access the account on approximately 14 occasions.

ii. IP addresses serviced by Servicio Di Telecomunicacion Di Aruba (Setar) N.V. (the telecommunications company in Aruba) were utilized to access the account on approximately ten occasions. The records identified that these IP addresses were utilized to access the account during the following approximate time periods: June 22, 2021 through June 27, 2021; December 16, 2021 through December 21, 2021 (which is consistent with the IP logs for the [redacted] account); and February 7, 2022 through February 8, 2022.

iii. Various IP addresses serviced by the Verizon cellular telephone network were utilized to access the account on approximately 189 occasions.

iv. Various other IP addresses serviced by other providers were utilized to access the account on a limited number of occasions.

Other Records

68. As part of another federal investigation, an agent from another federal law enforcement agency obtained records from American Airlines for flights taken by [redacted] These records identified the following (among other flights):

a. On or around December 15, 2021, [redacted] flew via American Airlines from the Dayton International Airport (in Ohio) to the Charlotte Douglas International Airport (in North Carolina) to the Queen Beatrice International Airport (in Aruba). On or around December 21, 2021, [redacted] flew via American Airlines from

the Queen Beatrice International Airport to the Charlotte Douglas International Airport to the Dayton International Airport.

i. As noted above, IP addresses serviced by Servicio Di Telecomunicacion Di Aruba (Setar) N.V. were used to access the [redacted] account and the [redacted] email account during the approximate time period of December 16, 2021 through December 21, 2021. The travel taken by [redacted] in December 2021 to Aruba is consistent with the use of these IP addresses.

b. On or around March 30, 2022, [redacted] flew via American Airlines from the Dayton International Airport to the Charlotte Douglas International Airport to the Queen Beatrice International Airport.

69. Based on American Airlines' records, the IP logs for the [redacted], and the IP logs for the [redacted] email account, it appears that [redacted] periodically travels to Aruba.

70. Records from the Ohio Bureau of Motor Vehicles identified that [redacted] utilizes the SUBJECT PREMISES on his current Ohio driver's licenses. Records from the Ohio Bureau of Motor Vehicles also identified that [redacted] has approximately six motor vehicles registered to him at the SUBJECT PREMISES.

71. Review of records from the Preble County, Ohio Auditor's website identified that [redacted] is the current sole owner of the SUBJECT PREMISES. The records identified that [redacted] has owned the SUBJECT PREMISES since in or around April 2018.

Internet Searches

72. On or around March 25, 2022, an FBI investigator searched publicly available information on various social media websites and messenger applications for any possible accounts associated with the email address [redacted] and the telephone number [redacted]. Among other accounts, the analyst located the following:

a. [redacted]

b. [redacted]

c. A Dropbox account was located that was associated with the email address

[redacted]

d. An Apple account was located that was associated with the email address [redacted].

73. Based on Internet research, it appears that [redacted] currently owns or manages three businesses in [redacted]: an [redacted]. Internet research indicates that [redacted] was previously the owner and/or manager of four strip clubs doing business under the name of [redacted]. These strip clubs were operated in four locations: Myrtle Beach, South Carolina; New Orleans, Louisiana; Toledo, Ohio; and Baltimore, Maryland. Various news media articles were located that reported that law enforcement officers had the following contacts with these strip clubs while [redacted] was the owner and/or manager:

a. News articles identified that law enforcement officers executed search warrants at [redacted] in Baltimore, Maryland on two occasions in or around 2015. Articles identified that the Baltimore Police Department executed a search warrant at [redacted] and other nearby locations in or around March 2015 at the culmination of a five-month investigation leading to the indictment of nine individuals for drug and gang violence offenses. [redacted] told a news media representative that the doorman employed at [redacted] was arrested as part of this investigation. Articles also identified that the Baltimore Police Department and FBI executed another search warrant at [redacted] in or around June 2015 related to a human trafficking investigation.

i. FBI records identify that [redacted] was interviewed by FBI agents as part of the human trafficking investigation. [redacted] told agents that his telephone number was [redacted] (the telephone number associated with the [redacted] email account). No federal charges were filed against [redacted] or any other [redacted] employees as the result of this investigation.

b. News articles identified that in or around 2015, the Louisiana Office of Alcohol and Tobacco Control and the Louisiana State Police revoked the licenses of several strip clubs on Bourbon Street in New Orleans, Louisiana following a month-long undercover investigation of prostitution and drug offenses. An article noted that [redacted] was one of the clubs that had its license suspended. The article further noted that [redacted] was the manager of [redacted], but he declined to comment on the investigation to the news media.

c. News articles identified that in or around 2016, four individuals were arrested in Horry County, South Carolina for multiple sex crimes involving two four-year old children. Two of the individuals arrested were employees of [redacted] in Myrtle Beach, South Carolina, and one of the locations of the sexual assaults was identified

as being the [redacted] business location. Three of the four individuals were convicted of the offenses. New reports identified that subsequent to the arrests, a letter was sent by the City of Myrtle Beach to [redacted], in care of [redacted], informing him that his business license was being revoked.

d. In or around 2018, a news article was published regarding [redacted] in Toledo, Ohio. The article identified that in the year and a half that [redacted] was open, the Toledo Police Department documented 31 crimes at the location, including a murder, shooting, and drug trafficking. The building's owner was interviewed by the news media and identified that [redacted] had leased the building and opened [redacted]

74. Other than the report of the FBI's interview of [redacted], which is noted above in paragraph 73(a)(i), I have not reviewed any of the police reports related to the above noted investigations. It does not appear from the news articles and [redacted] criminal history that he was ever arrested or charged with any offenses related to the above detailed investigations.

Conclusion Regarding Accounts

75. Based on all of the information detailed in the Affidavit, I submit that there is probable cause to believe the following:

a. [redacted] is the user of the [redacted] account. [redacted] has used this Kik account to distribute and possess child pornography files.

b. [redacted] is the user of the [redacted] email account. He has used this email account to register his [redacted] account.

c. [redacted] is the user of the Google account associated with the email address [redacted]

d. [redacted] is the user of the Dropbox account associated with the email address [redacted]

e. [redacted] is the user of the Skype accounts with the user names of [redacted] and [redacted]

Evidence Available in Email and Social Media Accounts

76. In my experience, individuals often post information on their social media accounts about other electronic accounts that they utilize – including their email addresses, other social media accounts, and messenger accounts (including Kik and Skype). This information may

provide evidentiary value to child exploitation investigations in that they help in identifying other accounts utilized by the offenders in furtherance of their child exploitation activities.

77. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs (including Kik and Skype). I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

78. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs (including Kik and Skype) as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

79. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs (including Kik and Skype). Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

80. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims. Based on the use of the profile name of [redacted] for the [redacted] account, it appears that [redacted] has utilized an alias.

81. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by

users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

82. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography and child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

83. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

84. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

85. As detailed above, there is probable cause to believe that [redacted] has a Google account associated with the email address [redacted].

86. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.

87. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

88. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

89. As detailed above, Google Location History is an application in which Google utilizes various data such as cell site information and Wi-Fi routers to locate and geo-locate a cellular telephone device. Google collects and stores this data if the application is enabled by the user, either during the set-up of the device or through the device's settings.

90. Based on my training and experience, I know that location information from cellular telephones and Google accounts can be materially relevant in investigations involving child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place. Furthermore, data regarding the subjects' whereabouts as obtained from the location information can lead to the identification of the places where computer devices used in furtherance of the crime may be present.

Evidence Sought in Searches of Dropbox Accounts

91. Dropbox and other cloud storage services provide a means for individuals to store files. Based on the information detailed above, there is probable cause to believe that [redacted] has utilized a Dropbox account associated with the email address [redacted].

92. As detailed above, I know based on my training and experience that individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

93. Based on information received from Dropbox Inc., I know that Dropbox Inc. maintains basic subscriber information for its users, including usernames, email addresses, and the dates that they established their accounts. Dropbox Inc. also maintains payment information, including credit card numbers, when payments are made on the accounts. Such information can provide material evidence regarding individuals involved in child pornography offenses, because this information can help identify the subjects and determine what aliases and email accounts they utilize. In addition, the dates that the accounts were established can help in identifying the length of time that the criminal activities transpired.

94. In addition to maintaining the files themselves, Dropbox Inc. also maintains logs documenting various activities associated with its accounts. One such log maintains information about the account name, computer name, and dates that files were uploaded, deleted, and modified. Such information provides material evidence to child pornography investigations, as the information helps identify the computer devices utilized by the subjects and when and how the files were received.

95. Dropbox Inc. maintains various other logs for its accounts. One such log maintains IP addresses and devices utilized to access the account. Such information is important to child pornography investigations because it helps to establish the subjects' identities, what computer devices are utilized, where the subjects' computers are located, and when the criminal activities transpired.

96. Another log maintained by Dropbox Inc. for its accounts details information about files being shared by the user. In cases involving the trading of child pornography, information about the shared files can be useful in helping to identify the subjects' trading activities.

97. Dropbox Inc. maintains various information about the settings for its users' accounts. Such settings include information about computers and other devices linked to the accounts. Information about what computers and devices are utilized by the subjects is again materially important to child pornography investigations.

Conclusion Regarding Probable Cause

98. Based on all of the information detailed above, there is probable cause to believe that information associated with the following accounts may contain evidence of [redacted] child pornography offenses:

a. The email account [redacted]

b. The Google account [redacted]

c. The Kik account with the user name of [redacted]

d. The Dropbox account associated with the email address [redacted] and

e. The Skype accounts containing the user names of [redacted] and [redacted].

99. Preservation requests were served to MediaLab.ai Inc., Google LLC, Yahoo Inc., Dropbox Inc., and Microsoft Corporation USA for the above noted accounts.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

100. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require MediaLab.ai Inc., Google LLC, Yahoo Inc., Dropbox Inc., and Microsoft Corporation USA to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-5. Upon receipt of the information described in Section I of Attachments B-1 through B-5, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-5.

CONCLUSION

101. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located in the accounts described in Attachments A-1 through A-5, including the following offenses: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1).

102. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-5.

103. Because the warrants for the accounts described in Attachments A-1 through A-5 will be served on MediaLab.ai Inc., Google LLC, Yahoo Inc., Dropbox Inc., and Microsoft Corporation USA, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Special Agent Andrea R. Rinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 31st of March 2022

Peter B. Silvain, Jr.
United States Magistrate Judge

T JUDGE